Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

*** TRADOC Regulation 25-1**

16 September 2006

Information Management: Automation

Information Resources Management

Summary. This regulation establishes policy and assigns responsibilities for governance of information management (IM) and information technology (IT) for U.S. Army Training and Doctrine Command (TRADOC) organizations. IM/IT addresses the management of information as a resource, the technology supporting information requirements, and knowledge management enablers as a means to achieve a net-centric knowledge-based force. The scope of Chief Information Officer (CIO) responsibilities and management processes is delineated throughout this regulation.

Applicability. This regulation applies to all TRADOC organizations within the U.S. Army.

Suggested Improvements. The proponent of this regulation is the TRADOC CIO. Send comments and suggested improvements on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC, ATTN: ATIM-T, 84 Patch Road, Fort Monroe, VA 23651-1051. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal). Electronic mail address: atim@monroe.army.mil.

Availability. This publication is available solely via the TRADOC Homepage at http://www.tradoc.army.mil.

Table of Contents

***This regulation supersedes TR 25-73, TR 25-70, and TRADOC Pamphlet 25-72.**

Chapter 1
Introduction

1-1. Purpose. TRADOC is the creator and owner of much of the Army's authoritative information, e.g., training support plans and manuals, programs of instruction and courseware, doctrine, concepts, and lessons learned. TRADOC commands, centers, and schools are the proponent and authoritative data source for specific categories and subjects of Army information. Information fuels our ability to effectively execute our missions and functions for the Army and enables command and control in the organization. Information requires lifecycle management, enabling resources (hardware, software, skilled personnel), and processes to assure its availability and effective use.

1-2. Scope. This regulation establishes policy for IM, the supporting IT, and the enablers to Knowledge Management (KM) in TRADOC. IT includes any information system, component, equipment, services, collection of hardware and software, or similar products that TRADOC uses to access, collect, process, store, transmit, display, and disseminate information. IM is the planning, budgeting for, manipulating, and controlling of information throughout its lifecycle. KM enablers are the technologies and processes that support access to and exchange of relevant information.

1-3. References. Appendix A contains the required and related publications.

1-4. Explanation of abbreviations and terms. The glossary contains abbreviations and special terms used in this regulation.

1-5. Responsibilities.

a. The TRADOC CIO will–

(1) Establish policy for the management of information resources and the programming, funding, and acquisition of IM/IT equipment and services.

(2) Develop guidance and plans for managing IM/IT investment strategies. Advise the TRADOC Mission and Resources Board (MRB) and the TRADOC Senior Resource Committee (SRC) in the prioritization of IM/IT requirements for funding.

(3) Assist the Deputy Chief of Staff for Resource Management (DCSRM) in determination of appropriate use of Operation Maintenance, Army (OMA)/Other Procurement, Army (OPA) funding for IM/IT acquisitions. Review all OPA spend plans with an IM/IT component before submission and execution.

(4) Chair the TRADOC IM/IT Enterprise Review Board (ERB) and oversee its operation in accordance with (IAW) its charter.

(5) Manage the process for IM/IT acquisitions that require Headquarters (HQ) TRADOC approval to include requirements that will incur a recurring obligation, for example, long haul communications services, desktop video teleconferencing, monthly/yearly user fees, etc.

(6) Chair the TRADOC Enterprise Architecture Management Board (EAMB). Provide architectural guidance to all TRADOC organizations and compile command-wide information management and technical standards.

(7) Coordinate with Office of the Army CIO/G6, Network Enterprise Technology Command (NETCOM), and the Installation Management Agency (IMA) regarding provisioning of enterprise and common user IM/IT services.

(8) Manage the Command Information Assurance (IA) Program, per Army Regulation (AR) 25-2 and TRADOC Supplement 1, and the Army Networthiness process required for all IM/IT systems.

(9) Provide the Command Webmaster and Records Manager.

(10) Serve as the Designated Approving Authority (DAA) for information systems developed and maintained by TRADOC schools, activities, major subordinate commands (MSC), and centers except as noted in para 1-5h.

b. The HQ TRADOC Deputy Chief of Staff for Operations and Training (DCSOPS&T) will incorporate IM/IT processes and requirements outlined in this regulation into the development of training, education, and leader development strategies and programs and will designate members to the TRADOC IM/IT ERB and EAMB as prescribed by their charters.

c. The HQ TRADOC DCSRM will—

(1) Centrally manage TRADOC's Planning, Programming, Budgeting, and Execution System (PPBES) activities to include procedures to obtain funds for IM/IT.

(2) Coordinate use of OMA/OPA with CIO prior to DCSRM decision. Review, approve, and submit Headquarters Department of the Army (HQDA) required OPA documentation.

(3) Coordinate management decision documents for all service contracts with an IM/IT component with the TRADOC CIO.

(4) Coordinate funding requests for projects that include IM/IT with TRADOC CIO for technical review and approval.

(5) Designate a member to the TRADOC IM/IT ERB as prescribed by the charter and integrate IM/IT ERB decisions into the MRB and SRC, as applicable.

d. Headquarters TRADOC Public Affairs Officer (PAO) will—

(1) Coordinate the TRADOC corporate information content and major themes on the TRADOC public homepage and pages linked off the TRADOC homepage.

(2) Serve as TRADOC web content manager for the TRADOC public web site. Approve for release new content posted on the TRADOC public web site.

(3) Coordinate with the TRADOC CIO on any content that may affect the supporting IT or conformance with policies related to IT.

e. TRADOC ARCIC will –

(1) Serve as proponent for the policies and procedures used by TRADOC organizations to acquire models and simulation systems.

(2) Coordinate with TRADOC CIO for architectural integration of those systems during requirements development.

(3) Designate a member to the TRADOC IM/IT ERB and EAMB as described by their charters.

f. TRADOC Commanders, Commandants, and Directors will —

(1) Establish processes and programs to effectively manage their information resources.

(2) Assign responsibilities to execute Army and TRADOC IM/IT policies and coordinate the management and operation of IM/IT to support mission requirements. This regulation refers to the assigned individual(s) for a TRADOC MSC or center as a CIO/G6 and at the school and activity level as an Information Management Officer (IMO). IMO responsibilities are detailed in DA Pamphlet (PAM) 25-1-1.

(3) Maintain accurate information on their IM/IT assets in the TRADOC CIO Architecture Repository (TCAR) for use in network readiness, investment management, and architecture development decisions.

(4) Prepare documentation regarding IM/IT acquisitions and comply with reporting requirements as stated throughout this regulation. Submit documentation to TRADOC CIO for acquisitions outside local approval authority.

(5) Develop and gain approval of IA certification, accreditation, and networthiness documentation prior to systems implementation.

(6) Coordinate with their supporting Directorate of Information Management (DOIM) prior to acquisition of any IM/IT that will be connected to the installation local or wide area networks.

(7) Establish procedures and assign responsibilities to manage the information/content life cycle in repositories, databases, portals, web sites, and shared drives.

(a) Assign responsibilities for the management and administration of command/activity public web sites.

(b) Assign an Army Knowledge Online (AKO) administrator to manage the command/activity AKO presence.

(8) Establish procedures and assign responsibility for records management per AR 25-400-2.

(9) Ensure Information Assurance Vulnerability Management (IAVM) compliance language is included in pertinent contracts and acquisitions.

g. U.S. Army Accessions Command (USAAC) operates the AAC Integrated Automation Architecture (IAA) in support of the U.S. Army Recruiting Command and U.S. Army Cadet Command and provides network support for U.S. MEPCOM and other USAAC mission areas. DA recognizes AAC's role as the single, centralized authority responsible for operating the enterprise-wide AAC-IAA. This authority is under the technical direction of NETCOM and the established procedures for the DA Human Resources Domain. AAC responsibility includes IAA operations, maintenance, sustainment, evolution, business decisions, and acquisition strategies.

(1) TRADOC authorizes USAAC to operate and maintain the AAC-IAA within existing Federal, Department of Defense (DoD), and DA guidance.

(2) AAC will designate a member to the TRADOC IM/IT ERB and EAMB as prescribed by their charters.

h. Staff Judge Advocates (SJA) at HQ and activity level will review materials, per requests from commands, units, or organizations, prior to posting on a public web site.

i. PAOs at activity level will—

(1) Review materials prior to posting on a public web site. Ensure content provider has coordinated with local operations security (OPSEC) officer and SJA for review prior to releasing information.

(2) Serve as web site content manager for the activity's public web site.

(3) Establish local procedures, in coordination with the local OPSEC officer, SJA, Deputy Chief of Staff for Intelligence, and webmaster, for review and clearance of information posted to the assigned TRADOC organization's web sites.

(4) Coordinate incorporation of TRADOC and local strategic communications themes into public web sites.

1-6. Other Army Organizations. TRADOC organizations will comply with policies, procedures, and standards established by the following organizations:

a. The Army CIO/G6 has statutory authority for the effective and efficient use of IT in the Army and exercises oversight for all IM/IT expenditures and investments. CIO/G6 approves the release of all OPA funds for IM/IT investments and the use of OMA funds for IM/IT acquisitions over the DA-determined threshold (currently $25,000) when funds are not allocated specifically for IT.

b. NETCOM, a direct reporting unit of the Army CIO/G6, provides strategic plans, standards, and technical guidance for the LandWarNet and all IM/IT managed at the enterprise level. NETCOM executes technical control over all IMA DOIMs.

c. IMA DOIMs provide architectural authentication and validation of IM/IT equipment or services connected to their installation networks. The supporting DOIM provides TRADOC organizations common-user baseline services as specified in the Command, Control, Communications, and Computer Information Management Services List and support as identified in specific service level agreements and memorandums of agreement.

d. The Army Contracting Agency (ACA) provides contracting policy and support to all Army organizations through installation Director of Contracting offices.

e. The Program Executive Office—Enterprise Information Systems negotiates and manages enterprise IM/IT contracts for hardware, software, and services.

f. DA-G2. Provides security guidance concerning content classification.

Chapter 2
Governance.

2-1. General. Planning for the effective and efficient use of IM/IT within TRADOC is not a "govern-once" activity that happens at the end of the fiscal year. Full cycle governance is an overall deliberate planning process that links sound IM/IT investments to enhanced mission planning and execution. Governance provides visibility of IM/IT spending and maintains focus on those activities that have the most strategic value to the command. IM/IT governance is an ongoing process of selecting, controlling, and evaluating solutions and starts with the identification of a functional need or requirement solution that can be enabled by use of IT.

2-2. Governance Structure. The TRADOC governance structure consists of the ERB, EAMB, and CIO subject matter experts.

a. ERB. The ERB serves as the executive body responsible for recommending enterprise IM/IT requirements and investments that are over $500K to the TRADOC Deputy Commanding General (DCG). The ERB, chaired by the CIO, reviews the business case for IM/IT investments over $500K to assess that the IM/IT initiative is aligned with TRADOC and Army strategic goals, supports maximum efficiency of TRADOC spending, and makes considered decisions about where IM/IT resources should be focused based on project/system risks, impacts, performance, and documented best business practices. IM/IT initiatives will be reviewed by the ERB via an electronic collaborative staffing process. The ERB will meet twice a year to discuss strategic direction for IM/IT in the command, prioritize unfunded IT requirements, and perform milestone reviews of existing investments. HQ TRADOC Deputy Chiefs of Staff, Commanders, MSCs and Director, ARCIC will designate a member to the TRADOC IM/IT ERB as prescribed by the charter. The ERB Charter is located on the TRADOC CIO IM/IT Reporting and Acquisition Decision (RAD) portal on AKO.

b. EAMB. The EAMB reviews and prioritizes initiatives and requests for new capabilities and upgrade/modernization requirements for IT that must satisfy TRADOC-wide requirements, affects military networks across or beyond TRADOC, or impacts existing Service Level Agreements in TRADOC. The EAMB looks at any requirement having these characteristics, regardless of anticipated cost. The EAMB consists of technical representatives from CIO, DCSOPS&T, Combined Arms Center (CAC), USAAC, ARCIC, Combined Arms Support Command (CASCOM), and Army Training Support Center (ATSC). Decisions and recommendations made by the EAMB may impact all TRADOC organizations. The EAMB will meet as needed, but as a minimum will meet twice a year in advance of the ERB. The EAMB charter is located on the IT RAD portal.

c. CIO Subject Matter Experts. The CIO staff reviews requirements and IM/IT solutions for policy and standards compliance, technical feasibility and integration, scope, cost, and impact on the network and architecture.

2-3. Governance Process (Diagram at Appendix B).

a. Requirements Submission. Sponsors submit their workplace and mission unique IM/IT requirements on TRADOC Form 25-1-E (RAD form) through their CIO/G6 or IMO. CIO/G6 or IMOs validate the requirement to ensure it meets organizational goals and forwards to the TRADOC CIO. The RAD form is a fillable template located on the IT RAD portal on AKO https://www.us.army.mil/suite/page/205769.

b. CIO Review. CIO staff will contact the submitter of the requirement, as necessary, and meet to discuss ongoing issues concerning submitted requirements. The CIO staff validates and/or determines the best technical solutions for requirements or, based on the scope and/or cost of the requirement, will approve, disapprove, or make a recommendation that CIO will forward to the EAMB or ERB. The CIO goal for disposition of requests is 5 days. However, requirements with a high $ value (exceeding $250K) or requirements that require more detailed evaluations, assessments, or testing by technical subject matter experts may not meet the preferred 5-day disposition window.

c. Disapproval. If the requirement is disapproved, the submitting organization will be notified by the CIO Integration Directorate, via e-mail, within 2-working days of disapproval. The e-mail will contain information explaining the reason(s) for the disapproval. A requirement below the ERB threshold can be disapproved at any level of the governance structure. Submitting organizations can appeal by sending an e-mail to their CIO/G6 or IMO and updating the RAD form with additional information to address concerns of the governance entities that reviewed and denied the request. The command/center CIO/G6 may coordinate with the TRADOC CIO to reevaluate the request.

d. Conflict Resolution. The TRADOC CIO will be the primary conflict resolution entity within the defined TRADOC IM/IT governance structure. The CIO will make the final decision on a below-threshold request and forward other requests to the ERB for review and endorsement. If the TRADOC CIO determines that a disapproved requirement should still be considered by the TRADOC ERB, the request can be included in the board's next meeting agenda. If an organization is not satisfied with the decision or results of the appeal, the issue may be resubmitted via the process described in para c. above.

e. EAMB Reviews. Recommendations for approval of initiatives and requirements from the EAMB will be submitted to the TRADOC IM/IT ERB for endorsement if the requirement exceeds the $500K threshold. If the requirement is below the $500K threshold, the decision will be made by the CIO. The EAMB may also recommend denial of a request/requirement based on votes cast by the board members. If a request is not recommended for approval, the EAMB will report that to the ERB through the CIO Integration Directorate. Decisions and recommendations made by the EAMB may impact all TRADOC organizations.

f. ERB reviews. The ERB will review and prioritize all requirements within their purview based on strategic alignment, risk, investment value, and performance management. The board will make appropriate changes and/or corrections to recommendations submitted and forward them to the TRADOC DCG. If a request is not recommended for approval, the CIO Integration Directorate will provide, in writing, the boards justification to the submitting organization.

2-4. Decision Baselines. TRADOC organizations will consider the following criteria when developing or assessing IM/IT solutions:

a. Security is a high priority and may be a more critical attribute than ease of use, accessibility, etc. when it comes to IM/IT use and purchase in TRADOC. Information systems must meet the approved DoD and DA security requirements as stated in AR 25-2 Information Assurance, with TRADOC Supplement 1.

b. Use of mandatory contracts and Army command license availability where applicable.

c. Compliance with published operational facilities (OPFAC) allocation guidance. Positions or facilities not covered by the OPFAC guidance will be addressed in organizational policy. OPFAC guidance is located on the IT RAD portal.

d. Expected benefit or other impact to functional processes and consistency with TRADOC Commanding General's (CG) priorities, e.g., as documented in TRADOC Campaign Plan, TRADOC Budget Guidance, Information Management Strategic Plan, and other documents.

e. Risk (e.g., technical difficulty to implement, user acceptance, immediacy and longevity of the benefits, compatibility with existing organizations and personnel skills.)

f. Compatibility with other planned or fielded IM capabilities in the command and on the installation.

g. Existence of like requirements and utility of a solution as a pilot for the initiation of a command-wide program.

h. Applicability of the solution for fielding beyond the target functional area (i.e., horizontal technology integration).

i. Compatibility with DoD or Army managed programs.

j. Consistency with standards in the Defense Information Standards Registry and the architectural guidance as published by the TRADOC CIO.

k. Return on investment and use of the appropriate category of funds (OMA and OPA).

l. Planning for and ability to sustain the system throughout its planned life cycle (i.e., hardware is purchased with 3-year maintenance contracts).

m. Ability to secure the information to be processed and stored.

2-5. Enterprise Solutions. TRADOC will capitalize on enterprise solutions, consolidated buys, and low cost/no cost solutions such as AKO to infuse our business processes with knowledge-based qualities, such as improved access to information and collaboration.

a. When applicable, capabilities will be optimized for the command vice the local level. Requirements common to multiple TRADOC organizations are best supported with a common enterprise solution that promotes standardization and a consolidated execution plan that promotes efficiency.

b. Standard solutions for similar requirements will be preferred over equal or slightly more capable unique solutions.

c. TRADOC relies on the installation DOIMs for infrastructure support and favors solutions that are DOIM approved and meet the minimum standard for mission execution.

d. TRADOC will use enterprise software agreements and hardware and services contracts managed by the Army Small Computer Program (ASCP) as its first source for IM/IT acquisitions for workplace and appropriate mission systems. Use of standard commercial off-the-shelf (COTS) products is preferred, when appropriate.

e. The Army Consolidated Buy (CB) Program consolidates Army requirements for desktops and laptops to get the best price for the enterprise and will be utilized by TRADOC organizations. Instructions for the CB, product descriptions, and detailed ordering procedures are posted on the ASCP web site https://ascp.monmouth.army.mil/scp/index.jsp.

2-6. Reporting Requirements. Proponents of IM/IT based systems have various reporting requirements for DoD, Army, and TRADOC. Details and links to mandatory IM/IT reporting requirements below can be found on the IT RAD portal site on AKO (https://www.us.army.mil/suite/page/205769).

a. Army Knowledge Management (AKM) Goal 1. TRADOC organizations must obtain a waiver from HQDA CIO/G6 to use non-IT programmed funds for the purchase of all IM/IT goods and services over $25K OMA and $100K Research, Development, and Acquisition. Thresholds are cumulative and IM/IT expenditures include all hardware, software, development, services, contractor support, testing, licenses and maintenance fees, web site and portal expenses, audio visual, and communications capabilities.

b. Army Portfolio Management Solution (APMS) – Army Information Technology Repository (AITR). The AITR is the Army's single, authoritative registry for IM/IT systems and is a module in the APMS. IM/IT systems must be entered in APMS-AITR if they meet criteria published in the Army Knowledge Management Guidance Memorandum - Capabilities-Based IT Portfolio Governance Implementing Guidance posted on the IT RAD portal. TRADOC system proponents enter system data and congressionally mandated reporting requirements through APMS-AITR:

(1) Federal Information Security Management Act (FISMA) mandates that the security status of Army information systems be documented, updated, and verified at least annually. Security requirements are specified in AR 25-2. System proponents will use AITR to report FISMA compliance. FISMA guidance and mandates are posted on the IT RAD portal on AKO.

(2) Business Management Modernization Program (BMMP). DoD requires certification of defense business systems costing over $1M. If a system requires $1M or more in modernization costs, the Army Domain Lead may require additional data in APMS. To determine the systems that meet the criteria for reporting go to http://www.dod.mil/bmmp/faq_certification.html.

2-7. Strategic Planning. Planning for the effective use of IM/IT is an ongoing activity and the responsibility of every commander/director within TRADOC. IM/IT plans provide the commander visibility over IM requirements and assist the TRADOC CIO in enterprise planning and acquisition, standards application, and overall fiscal responsibility. The TRADOC IM/IT Strategic Plan (IMSP) lays out the strategic direction and priorities of IM/IT in the command and will be updated by the TRADOC CIO annually.

Chapter 3.
Capital Planning and Investment Management.

3-1. Portfolio Management Overview. The primary goal of IM/IT Capital Planning and Investment Management is to prioritize IM/IT spending across TRADOC functional proponents by assessing and managing IT as a portfolio of investments. The APMS is the Army's primary portfolio management decision support tool. Effective portfolio management ensures that IM/IT investments support the Army's mission, vision, and goals; ensures an efficient delivery of capabilities to the warfighter; and maximizes return on investment to the enterprise. APMS assists TRADOC CIO in identifying potential redundant or inefficient systems for consolidation or elimination, while supporting budgeting decisions.

3-2. Developing a Business Case. The business case defines the purpose and expected outcome of the initiative. A business case is used by the TRADOC CIO and ERB to assess the value of proposed IM/IT projects (initiatives) and make a recommendation on funding and priority. The level of detail required for the business case is in direct

relationship to the cost of the initiative. A fully developed business case includes the purpose, costs, recommended solution, operational impact, risk assessment, funding plan, milestones, and performance measures. TRADOC IM/IT acquisitions or initiatives costing $500K or more over the project lifecycle will have a fully developed business case and must be sponsored at the O6/GS15 level.

3-3. Milestone Reviews. Initiatives costing more than $500K over their lifecycle must include annual milestone reviews during the development stage and after implementation, during sustainment. The ERB will conduct a review to assess the accuracy of cost estimates and implementation timelines, the satisfaction of business users with the results of their investment, the achievement of benefits that were stated, and to gauge whether any lessons were learned. The annual milestone review meeting of the ERB will be in the first quarter of the fiscal year.

3-4. Submitting Capability Requests. TRADOC organizations with a business requirement that do not have a recommended technical solution may request CIO assistance using the RAD form. In the 'Category of Request' box on the RAD form, select 'Initial Concept'. CIO will work with the submitting organization to build the appropriate level of business case and identify the best solution to meet the requirement.

3-5. Resource Management. HQ TRADOC DCSRM manages all requirements throughout the PPBES cycle and the accompanying current and budget year unfinanced requirements (UFR) process, to include requirements that depend upon IM/IT for their total or partial solution. DCSRM coordinates with TRADOC CIO regarding the validity, architectural conformance, duplication, and priority of requirements for IM capabilities. CIO coordinates with TRADOC organizations to clarify, consolidate, or deconflict requirements they have submitted to DCSRM for funding consideration in the web-based TRADOC Automated Schedules (WebTAS). TRADOC CIO recommends strategies for integrated management of IM/IT investments to the ERB.

3-6. Types of Funds. The two categories of funds that generally fund IT are OMA and OPA.

a. OMA is used if the cost of an IM/IT system is below the investment threshold mandated by public law (currently $250K). Acquisitions will not be fragmented to stay below this threshold for a system.

b. OPA is used if the cost of an IM/IT system exceeds $250K and should be programmed 2 years out in the POM.

c. IAW Defense Finance and Accounting Service-Indianapolis Center (DFAS-IN) Manual 37-100-XX (XX=FY), Appendix A, an IM/IT system exists if a number of components are designed primarily to function within the context of a whole and will be interconnected to satisfy an approved Army requirement. This appendix also provides guidance on what should be included when calculating the total cost of a system to determine if IM/IT exceeds the OMA/OPA threshold.

3-7. Validated UFRs. UFRs entered into WebTAS are generally not written with the specificity required for approval of IM/IT acquisitions. Therefore, the requiring activity must complete a RAD form prior to CIO consideration of the UFR.

3-8. IM/IT and Telecommunications Requests. Requests for acquisition of IM/IT are submitted on the RAD form and the governance processes previously described in chapter 2, para 2-3 apply. Services related to IM/IT are considered as part of the oversight requirement of this regulation.

a. Requiring activities must obtain TRADOC CIO approval via the RAD form for acquisition of IM/IT that meets any of the following criteria:

(1) All software development initiatives and COTS modifications.

(2) All server hardware and software, network, wireless, and security devices.

(3) All collaboration software and any other software not on TRADOC's recommended product list.

(4) Any software, hardware (including maintenance), and services not being purchased using mandatory ASCP contracts or that do not have an ASCP waiver.

(5) Radios that are associated with an installation Land Mobile Radio (LMR) program (tactical radios do not need to be reported).

(6) Any hardware, software, IM/IT initiatives, or services with a cumulative cost above $25K.

(7) Commander TRADOC delegates approval authority up to $1M to USAAC for acquisitions in support of the AAC IAA. Above this threshold, the approval procedures in this regulation apply. USAAC will submit a quarterly expenditure report to the TRADOC CIO for IT acquisitions $25K - $1M, which will be incorporated into the IM/IT governance report provided to the DCG.

b. The following are examples of items that are not reportable as long as the total acquisition cost does not exceed $25K, purchase is not restricted by annually published budget or DA guidance, applicable items are purchased from ASCP contracts, and is within the published OPFAC allocation guidelines:

(1) Printers, scanners, faxes, copiers

(2) Monitors, mouse and/or keyboards

(3) Memory or expansion/controller cards

(4) Uninterruptible power supply

(5) Audiovisual equipment.

(6) Individual end-user devices such as a laptop or desktop computer for a new employee or to replace a failed system.

c. TRADOC CIO acquisition guidance does not apply to the following:

(1) Consumables or general supply/support items, i.e., compact discs, digital video disks, tapes, ribbons, diskettes, ink/toner cartridges, bulbs, publications, cables, thumb drives, carrying cases, and print wheels. Local IM/IT policy will address these items.

(2) Automated components embedded as part of a weapon system, medical instrumentation, and servomechanisms that do not interface or communicate outside the host tool, system, or device. These systems must meet DA and DoD reporting requirements.

d. IM/IT Acquisition and Capability and Approval Threshold Chart (Table 3-1).

Table 3-1
IM/IT Acquisition and Capability and Approval Threshold

Criteria	Approval levels*	Required Documentation **	Authority
Acquisition is < $25K and meets criteria in paras 3-8.b or 3-8.c above	Activity CIO/G6 or IMO	Local determination	Local Determination
Acquisition is <$25K and meets criteria in para 3-8.a above	TRADOC CIO	IT RAD Form 25-1-E and HQDA documentation for AKM governance	This regulation and AR 25-1
Acquisition is >$25K and <$500K	TRADOC CIO	IT RAD Form 25-1-E and HQDA documentation for AKM gov.	This regulation and AR 25-1
Acquisition is >$500K	TRADOC DCG (w/ERB recommendation)	IT RAD Form 25-1-E and HQDA documentation for AKM governance	This regulation and AR 25-1
Defense business system modernization > $1M	TRADOC DCG (w/ERB recommendation) then HQDA	IT RAD Form 25-1-E and BMMP Certification	This regulation and DoD Directive
Collaboration Capability regardless of cost	TRADOC CIO then if >$25K HQDA	IT RAD Form 25-1-E and HQDA documentation for AKM governance	This regulation and AR 25-1
Server and/or server software regardless of cost	TRADOC CIO then HQDA	IT RAD Form 25-1-E	This regulation and AR 25-1
Classroom Hardware	TRADOC DCSOPS&T then CIO then (if > $25K) HQDA	IT RAD Form 25-1-E	This regulation and AR 25-1
Warfighting system or model or simulation	ARCIC then TRADOC CIO then HQDA	Initial Capabilities Document	AR 70-1, AR 71-9, AR 25-1

* CIO approval is not an authorization to connect to the installation network. TRADOC organizations will coordinate IT acquisitions with the supporting DOIM.
** DA Consolidated Buy and ASCP mandatory contracts apply.

e. Telecommunications. TRADOC CIO centrally manages TRADOC's long haul communication requirements. Long haul communications are any general or special purpose telecommunications leaving the installation, regardless of distance. USAAC CIO is authorized to manage telecommunications services for USAAC within their

allocated funds. TRADOC CIO will coordinate with organizations annually to validate long haul requirements.

(1) Long haul services are categorized in one of two ways: Defense Information System Network (DISN) or non-DISN.

(a) DISN subscription services include Defense Switched Network, Defense Red Switch Network, Joint Worldwide Intelligence Communication System (JWICS), Nonsecure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Defense Messaging System (DMS), Ground Surveillance Radar, Intelligence, Surveillance and Reconnaissance, Video Teleconference, and DISN transport services. DISN services are programmed for and paid by DA.

(b) Non-DISN long haul includes services for commercial and military satellite services, Global System for Mobile Communication, Federal Telecommunications Services, and Public Switch Telephone Network. Non-DISN services are programmed and paid for by TRADOC CIO.

(c) Start, Change, or Discontinue Long Haul Service. TRADOC organizations coordinate the provision of service with the supporting DOIM who enters the request through Defense Information Systems Agency Direct Order Entry (DDOE). Long haul service requests specific to TRADOC mission support (whether DISN or Non-DISN) are automatically routed through TRADOC CIO for approval by the DDOE web application. New DISN services must be paid for by TRADOC in the year of execution until programmed by DA. New non-DISN services are added to the program requirements by TRADOC CIO.

(2) Cell Phones and Personal Digital Assistants (PDAs). AR 25-1 and AR 25-2 govern policies and procedures for cell phones and PDAs (e.g., BlackBerry devices). Commanders or directors must have a program in place to actively manage the use of wireless technology to include:

(a) Developing local allocation priorities in accordance with OPFAC guidelines located on the IT RAD portal on AKO.

(b) Coordinating with the local DOIM to identify contract vehicles that best support mission requirements and limit the total cost of ownership. Information regarding the blanket purchase agreements (BPAs) can be found on the ACA, Information Technology E-Commerce and Commercial Contracting Center's webpage: http://www.itec4.army.mil under Master Contracts, Wireless Handheld BPAs.

(c) Assigning responsibilities for reviewing expenditures and usage, and evaluate opportunities for resource sharing, use of aggregate purchases, and pooling of minutes.

(d) Implementing ongoing asset tracking and inventory control of these devices using the TCAR.

f. Copiers. AR 25-30, governs the policies and procedures for self-service copying management. Requests for copiers are submitted via the RAD form and OPFAC allocation guidelines apply. TRADOC organizations will utilize installation copier contracts if available. Copiers are reported in the TCAR.

3-9. Contracts.

a. Contracts supporting IM/IT based systems must include wording that requires compliance with Army IA requirements, such as system certification, accreditation, and networthiness; training and certification of IA personnel; and IAVM compliance. These requirements must be included in mission needs statements, operational requirements documents, capstone requirement documents, statements of work, and all other system acquisition, contracting, and development documents.

(1) TRADOC contracts will require all software or systems developed for use on the Army Enterprise Infostructure (AEI) to meet minimum security standards stated in AR 25-2 and other DA and DoD policies, to include IAVM compliance, patch management, and the use of antivirus and other IA software.

(2) All information systems developed or acquired must meet DoD and DA certification, accreditation, and/or networthiness requirements before being connected to the AEI.

(3) Contractor nominated personnel must meet all IA training and certification requirements in AR 25-2, DoD 8570.01-M, and the Army's IA Training Best Business Practice before acceptance for employment. Additionally, contractors must maintain Army IA training and certification compliance throughout the contract period at no expense to TRADOC.

(4) Contractor nominated personnel must meet security clearance requirements specified in AR 25-2 before acceptance for employment. Contractors must maintain their security clearances throughout the contract period at no expense to TRADOC.

(5) Contractor access to information residing on a government information system (IS) or network will be limited to that required to fulfill the terms of the contract.

(6) Contractor owned and operated IS will meet all security requirements for government owned hardware and software when operating on the AEI or conducting official business.

b. In accordance with DA PAM 25-1-1, IT Support and Services, 20 Mar 2006 para 9-1b. - all COTS IT hardware and software (to include maintenance) and services must be purchased from ASCP contracts that include the DoD and SmartBUY Enterprise

Software Agreements (ESA). If the requirement cannot be fulfilled via these contracts, request a waiver from ASCP at https://ascp.monmouth.army.mil/scp/waiver/wv_index.jsp. The ASCP process is for government personnel to submit IT purchases from their contracts. Turn-key services contracts, initiated by or for TRADOC, will not include tasks and related dollars for the contractor to purchase COTS IT hardware or software. If the ASCP Office preferred purchasing process cannot be met:

(1) The Contracting Officer for the services contract must write an authorization letter to authorize the contractor to purchase COTS IT from the ASCP contracts on behalf of the government.

(2) The contractor must have an AKO login to access the ASCP site.

(3) The contractor must be able to make the specific types of payment required by the ASCP contracts such as delivery order, credit card, or check.

(4) Use of a contractor for purchase of COTS IT does not void the requirement for TRADOC and Army mandated approvals before the actual purchases are made.

c. Contractors must abide by local installation policies for network and telephone access. Contractor equipment cannot be connected to the NIPRNET or SIPRNET without supporting DOIM approval. Contracts requiring access to government furnished equipment must state that local installation policies for internet access will be met.

Chapter 4
Enterprise Architecture.

4-1. General. The enterprise architecture (EA) provides a blueprint for how TRADOC executes its mission--documenting the processes for how core functions are accomplished, the systems that support those processes, and the technical standards. The EA contains both the current baseline 'As-Is' state and target 'To-Be' state. The EA provides standardization of decision making related to capability delivery; however, IM/IT is constantly evolving based on emerging operational requirements and technology advances. TRADOC EA follows the DoD Architecture Framework depicting an operational, systems, and technical view. The value of the EA to the local IM/IT decision maker is to define the business, application, infrastructure, and information configurations that are currently in place. Reuse of and integration into existing standards is a more effective and efficient way to design solutions to support a network-centric, knowledge-based operation.

4-2. Command Architecture. The command architecture includes operational, systems, and technical views for TRADOC core functions (as defined in TR 10-5) and its

command and control. Command architecture development is a collaborative effort between the core functional leads and the CIO. CIO ensures the integration of the command architecture with Army and joint systems and standards.

4-3. Enterprise Architecture Plan (EAP). The EAP is the execution component of the IMSP and is a consolidated plan for enterprise IM/IT-related efforts. IM/IT is a collaborative effort between the leads for TRADOC core functions and the HQ staff that lays out the rate of modernization in manageable increments to accommodate mission priorities, level of effort and risk, funding streams, and execution responsibilities. CIO will publish the EAP annually and post to the IT RAD portal.

4-4. TRADOC CIO Architecture Repository (TCAR). The TCAR is the portal (located at https://collab.tradoc.army.mil/itarch/) bringing together architecture views depicting the alignment of business processes with their information management requirements and the management of IM/IT assets. TRADOC CIO office and activity IM/IT personnel use the TCAR as a basis for resource management and predictive analysis. TCAR can be accessed from any military or government domain (.mil or .gov) by using Internet Explorer. User roles associated with the TCAR include approval authorities found at the installation and MSC levels, activity and sub-activity authors found at the MSC level and below, and read only access available at any level in the command structure. Potential users request access via a feature on the TCAR portal, thereby sending an e-mail to the respective approval authority who endorses their admission to this repository.

a. The IM/IT asset management module of the TCAR provides consolidated storage and presentation of data regarding TRADOC's IM/IT resources and architecture related information for use in current and future IM/IT management. The TCAR is available at any time enabling activity and sub-activity authors to update their data as needed. Activity/sub-activity authors certify their data as being complete and accurate three times annually followed by approval authorities verifying subordinate activity/sub-activity author certification within their span of control. Critical pieces of information for each item in the repository have been designated as the minimum essential requirements for the certification process. These data fields must be completed prior to installations, MSC, and their subordinate organizations to finishing TCAR certification. When attempting certification, any information missing from these key fields causes an error message listing the missing data elements. Activity/sub-activity authors must provide this information before receiving a certification accomplished notice from the TCAR.

b. The TRADOC CIO office maintains command architecture products in the TCAR.

c. Activity/sub-activity authors enter and certify information pertaining to data repositories (i.e., databases, web sites, portals, shared drives, etc.) in the TCAR as items of particular command interest. System owners will list information exchange requirements for repositories and content stores in TCAR and will identify the organization responsible for protecting and controlling access to this data.

4-5. Operational Facilities (OPFAC) Allocation Guidelines. Commanders use the OPFAC guidelines as the baseline for IM/IT allocations. The EAMB generates OPFACs consisting of a set of guidelines that define functional elements (i.e., a generic duty positions such as action officer or senior executive, or a place such as a conference room) and apply assignment rules, allocation rules, and IM/IT requirements descriptions corresponding to each functional element. Current OPFAC guidelines are available on the AKO IT RAD portal. The following useful planning tools are available via the TCAR graphic interface: The OPFAC Rules Summary providing recommended asset densities, personal computer costs, other IM/IT device costs, and total costs associated with individual functional elements.

4-6. Standards. CIO will publish a consolidated list of policy and standards, TRADOC's catalogue of services, and recommended product lists on the AKO IT RAD portal. TRADOC organizations will use these services and products to fulfill requirements. Exceptions will be submitted using the RAD form and must be approved by the CIO or the EAMB as appropriate.

Chapter 5
Knowledge Environment.

5-1. General. The knowledge environment concerns the information TRADOC requires to execute its missions in support of the Army and the DoD. The requirements for content management and web design contained in this chapter also apply to the TRADOC public web presence.

5-2. Collaboration Capabilities. The DoD and Army place extra conditions on the management of collaboration capabilities and CIO enforces these requirements for TRADOC mission collaboration needs. Collaboration capabilities enable two or more individuals who are not collocated to use an electronic environment to communicate, plan, coordinate and make decisions. They include, for example, voice and video conferencing; text, document, and application sharing; awareness and instant messaging; and whiteboarding. CIO develops and maintains TRADOC's architecture for collaboration capabilities and coordinates the service delivery responsibilities. CIO advises TRADOC organizations on solutions for their unique collaboration requirements and approves the acquisition of new collaboration capabilities, regardless of cost. TRADOC organizations will:

a. Utilize existing solutions such as AKO, TRADOC Knowledge Environment (TKE) and Battle Command Knowledge System (BCKS).

(1) AKO (https://us.army.mil) is the Army's intranet and the preferred collaboration capability.

(2) TKE is a TRADOC-hosted portal that provides close integration with MS Office products to enhance organizational productivity

(https://tke.army.mil/default.aspx). TKE site owners can authorize foreign officials and students assigned to TRADOC access to TKE.

(3) BCKS provides a network of structured professional forums (SPF) focused on knowledge transfer and leader development (https://bcks.army.mil). Creating a SPF community on BCKS provides a complimentary capability to the training and leader development mission of the schools.

b. Utilize DoD and Army approved products and contracts, https://ascp.monmouth.army.mil/scp/index.jsp, and TRADOC-specific extensions of these.

c. Obtain certifications or waivers at the required level for alternative solutions IAW current guidance on the Employment of Collaborative tools https://www.us.army.mil/suite/doc/5747635.

d. Propose modifications to enterprise collaboration capabilities, e.g., AKO and TKE, via the TRADOC CIO representative to the configuration control boards.

5-3. Content Management. Access to relevant content is the underpinning of the knowledge environment. TRADOC organizations with web pages, portals, repositories, and shared drives will adhere to the following policies to maximize the security and accessibility of their content.

a. Storage. AKO is the preferred access point and storage for content. TRADOC organizations will not use e-mail to transmit large files and attachments and will comply with size limitations identified by local DOIM's. Sharing of large files should be done using AKO files, TKE, or other secure file sharing environment. TRADOC activities are authorized to store content in a variety of repositories:

(1) AKO Files. All organizations listed in TRADOC 10-5 will have a Knowledge Center on AKO and use it for content that must be available to the Army community. TRADOC CIO determines the AKO organizational file structure at the Army command level. Each top level organizational community in TRADOC will create at least one Knowledge Center and public folder that is searchable and accessible to all official personnel.

(a) Public Folders. The AKO public folder only includes content that is available to all official personnel and for which the organization is the proponent and release authority.

(b) Workgroup/Limited Access Folders. These folders are managed by the folder owner who grants access to users or groups based on mission requirements. These folders may be used for copies of official documents or publications needed on a temporary basis by the members of the group. Copies will be deleted by the folder owner when no longer needed.

(2) TRADOC Shared Drives. Shared drives do not support a net-centric architecture and TRADOC activities will make limited use of them only as required for local and temporary processes. Authorized uses include as records management archives, web development environment, or for short term storage when transferring content.

(3) Databases. TRADOC database owners will not duplicate the content of an authoritative source. CIO maintains procedures to register federated databases in TCAR. Federated database owners will coordinate new or changed database systems with CIO.

(4) Web sites and Portals (including TKE, AKO and BCKS).

(a) TKE is appropriate for development and sharing of internal TRADOC/ organizational content. TKE content is web-accessible.

(b) Content on web sites and portals will be linked to the authoritative source, rather than copied or duplicated on that site.

(c) Content on public web sites must be approved for release by the PAO.

(d) All non-public content will be on a site that is accessible through AKO authentication, common access card authentication, and/or restricted by user name and password.

b. Content Security. Data owners must determine the level of accessibility for their content - i.e., public or limited. Working draft content will not be stored in publicly accessible files or portals.

(1) The following sources and types of information must not be made publicly accessible:

(a) Training support plans, mission training plans, drills, field manuals, tactical vignettes, and other material that describes how Soldiers perform functions in the U.S. Army. Examples include small unit tactics patrolling, stability and support operations, engineer operations, aviation operations, logistics procedures, and systems capabilities.

(b) Specific vulnerabilities to operations, equipment, or personnel, including, but not limited to, force protection, significant troop movements, readiness data, and tactics, techniques, and procedures (TTP).

(c) Lessons learned, formal and informal TTP, and "how-to" articles that deal with topics described in paragraphs (a) and (b) above.

(d) Press releases that detail how Soldiers are accomplishing the mission.

(e) Information relating to the funding, fielding, vulnerabilities, and capabilities of new equipment.

(f) Classified information is to be secured IAW AR 380-5 and not to be made accessible from any UNCLASSIFIED server or web site, to include private web sites or portals.

(2) Unclassified critical and sensitive operational traffic that specifically includes information about "shortfalls in training" due to funding, general officers' overseas travel schedules, and deployed/deploying troops will be transmitted over a secure network. TRADOC organizations will use the following guidance regarding the classification and transmission of operational data:

(a) Data classified as "For Official Use Only" will, at a minimum, be signed using common access card/public key infrastructure (PKI).

(b) Data classified as "Sensitive but Unclassified" will, at a minimum, be signed and encrypted using common access card /PKI.

(c) Data classified as "Confidential" or "Secret" will be transmitted over a network with a minimum security classification of Secret (e.g., SIPRNET, JWICS).

(3) TRADOC centers, schools, and activities will periodically review their secure network capabilities to ensure they are capable of implementing the above guidance. TRADOC organizations will coordinate with their supporting DOIM regarding access to classified long haul networks available as common user (non-reimbursable) services. TRADOC organizations will report additional requirements for secure network capabilities to the TRADOC CIO using the RAD form.

c. Content Discoverability. TRADOC organizations will implement Army policies regarding the organization of content and its discoverability, e.g., standard metatags and taxonomies.

(1) TRADOC organizations will use the DoD mandatory discovery metadata elements for resources posted to community and shared spaces as identified in the Department of Defense Discovery Metadata Specifications (DDMS) (Appendix C). The DoD Metadata Registry and Clearinghouse is a catalogue of XML schemas, taxonomies, reference data sets, and data elements. Metadata schemas and taxonomies for TRADOC content that need to be accessed across the DoD enterprise will be registered in the DoD Metadata Registry and Clearinghouse https://metadata.dod.mil/mdrPortal/appmanager/mdr/mdr.

(2) The CIO maintains a catalogue of current taxonomies used in TRADOC and oversees the integration of taxonomies used to organize TRADOC's information content. TRADOC's baseline taxonomy to categorize warfighter content is the Army Universal

Task List (AUTL) (FM 7-15). Other TRADOC taxonomies that categorize warfighter content will integrate and/or map to the AUTL for maximum discoverability.

(3) TRADOC organizations will utilize the Sharable Content Object Reference Model (SCORM) when developing learning content. SCORM is a suite of technical standards that enable web-based learning systems to find, import, share, reuse, and export learning content in a standardized way. SCORM is written primarily for vendors and toolmakers who build learning management systems and learning content authoring tools so they know what they need to do to their products to conform with SCORM technically. For details on SCORM, access the following URL http://www.adlnet.gov/index.cfm.

5-4. Records Management. TRADOC commanders will establish a records management program IAW U.S. Code: Title 44, Chapter 31. Records management applies to the entire lifecycle of official records from creation through final disposition. Official records include all documentary materials, regardless of physical form or characteristics that provide evidentiary accounting for decisions, policies, plans, organizations, functions, procedures, operations, and essential transactions of an organization. It is the originating organization's responsibility to determine the record status of information and manage it appropriately. TRADOC organizations must implement Army policies regarding the management of official records per AR 25–400–2. The Army Records Information Management System (ARIMS) is a web-based tool to manage both hardcopy and electronic Army records.

a. TRADOC Records Management Duties and Responsibilities (see Table 5-1)

Table 5-1
TRADOC Records Management Duties and Responsibilities

TITLE	APPOINTED LEVEL	DUTIES AND RESPONSIBILITIES
Records Administrator (RA)	**TRADOC CIO**	An individual who is appointed in writing and serves on the Army Command or Army staff (ARSTAF) with command-wide records management program responsibilities. RAs have approval authority for AOs and RCs requesting RM or RHAM privileges. RAs may approve Office Records List (ORLs) and serve as points of contact (POC) for the access and release of stored records for which they are responsible. (See para 8-2g(3), AR 25-1).
Records Holding Area Manager (RHAM)	**Garrison**	An individual whose duties include managing and directing the operations of a records holding area facility. RHAMs may also possess the same duties and access privileges as a Records Manager if they have been approved by their Army Command Records Administrator (RA). (See para 8-2g(7), AR 25-1).
Records Manager (RM)	***MSCs, Special Activities, Centers and Schools**	An individual who serves at the subordinate command level or on the installation garrison staff with command-wide or garrison-wide records management responsibilities. RMs have approval authority for AOs requesting RC privileges. RMs also approve proposed Office Records Lists (ORLs) and serve as points of contact (POC) for the access and release of stored records for which they are responsible. (See paras 8-2g(4), 8-2g(6), and 8-2g(7), AR 25-1).
Records Coordinator (RC)	**As needed to assist RMs**	RCs are responsible for providing Records Management services to one or more unit(s)/office(s) and act as liaison between the unit(s)/ office(s) and the servicing RM and Records Holding Area Manager. They also serve as points of contact (POC) for the access and release of stored records for which they are responsible. (See para 8-2g(8), AR 25-1).
Action Officer (AO)	**As needed to meet needs of individual organization**	AOs are responsible for managing the records they create on behalf of the Army that are used for their unit/office level business operations. An AO can use ARIMS to create a proposed Office Records List (ORL) to categorize the records created in his/her office. (See para 8-2g(9), AR 25-1).

***Coordinate with TRADOC Records Administrator for additional RMs to support the needs of the organization.**

b. E-mail has become a primary means of communicating decisions, policies, plans, procedures, and other essential information regarding government business; and, therefore must be preserved. E-mail, identified as records, must be managed, protected and retained as long as needed for ongoing operations, audits, legal proceedings, or

research IAW AR 25-400-2 and ARIMS Record Retention Schedule-Army. Individuals originating the e-mail will determine the record status of their e-mail.

(1) E-mail records might include: Policies and directives; correspondence or memoranda related to official business; work schedules and assignments; agendas and minutes of meetings; drafts of documents that are circulated for comment or approval; any document that initiates, authorizes, or completes a business transaction; and final reports or recommendations.

(2) E-mail records identified with retention of 6 years or less are designated as keep ("K") records and managed locally through the life cycle. E-mail records identified with retention longer than 6 years are to be designated as transfer ("T") records and transferred to the ARIMS Army electronic archive records repository. These records will be further managed and disposed of at the end of their life cycle or transferred to the National Archives and Records Administration as a permanent record.

(3) The following examples are generally not considered in the category of e-mail records: Personal messages and announcements not related to official business; copies of extracts of documents distributed for convenience or reference; and announcements of social events (e.g. retirement parties or holiday celebrations).

c. Per AR 25-11, paragraph 13-3a, routine, unclassified organizational record information may be sent in memorandum format as an attachment via organizational e–mail. Organizational e-mail accounts are the preferred method for passing official taskings, official requests, and official responses. Messages containing record information should be digitally-signed using the organizational e-mail account's PKI certificate. Organizations can obtain certificates for their organizational accounts from the Army Registration Authority, army.ra@us.army.mil. When using e-mail to transmit the record copy of correspondence, e-mail users will state the following in the e-mail note: THIS CORRESPONDENCE IS SENT TO YOU AS ORGANIZATIONAL ELECTRONIC MAIL IAW THE PROVISIONS OF AR 25-11. THIS IS THE OFFICIAL COPY. YOU WILL NOT RECEIVE A PAPER COPY.

5.5. Portal/Web Site Administration. This paragraph provides policy specific to creating and maintaining a TRADOC web site or portal. TRADOC activities will determine their local requirements to produce and maintain a site and coordinate their establishment with the CIO/G6 or IMO and appropriate webmaster. The person responsible for maintaining public web sites is known as the mission webmaster and the person responsible for maintaining a portal is known as the portal administrator. All TRADOC public sites must have a primary mission webmaster or portal administrator designated in writing by a commander/supervisor. All TRADOC public and private web sites, except those operating under the AAC-IAA, must be located on a .mil domain. Pre-existing Army web sites maintained in non-government domains (i.e., .org, .com, .net, and .edu) will execute plans to transition web sites to a.mil domain.

a. Mission Webmaster/Portal administrators will−

(1) Ensure sites comply with DoD web site administration policy, AR 25-1, and subsequent DoD and Army directives. Current policy can be found at http://www.defenselink.mil/webmasters/ and http://www.army.mil/webmasters/.

(2) Establish a process for the periodic review of their sites for security risks and design deficiencies.

(3) Ensure their web sites maintain a consistent look and feel and that all web pages clearly identify which web site the visitor is on.

(4) Monitor the accuracy of links on their web sites. At least monthly, mission webmasters will review error data in their web site's automated access logs and take action to correct link and document access errors.

(5) Complete the Online Army Webmaster Training Course located at https://iatraining.us.army.mil/index.php.

(6) Perform housekeeping functions such as monitoring file expiration and cleanup; and for limited access sites, deleting users who no longer need access to the portal.

b. All TRADOC sites must contain the following information:

(1) Links to:

(a) the next senior web site in the hierarchy IAW 10-5. For Example: The Command and Staff College should link up to the main CAC web site.

(b) the organizational home page on AKO (if one exists).

(c) the TRADOC logo and motto.

(d) HQ TRADOC home page http://www.tradoc.army.mil/.

(e) Army home page: http://www.army.mil/.

(2) Description of (or link to) local mission statement and organizational structure (excluding names of personnel).

(3) Contact information for the mission webmaster/portal administrator, at a minimum, the mission webmaster/administrator e-mail address for users to request information or direct questions, comments, suggestions, etc. to for that organization.

(4) Links to non-government web sites must directly support the mission and not imply endorsement of products or services.

(5) A statement indicating "This is an official U.S. Army site."

c. Public Sites. Public sites are developed when an organization wishes to provide all users with information. There are two types of public sites – TRADOC public web sites and AKO organizational portals.

(1) TRADOC Public Web Sites. Organizations will coordinate the establishment of new web sites and Uniform Resource Locators (URLs) with the next higher level webmaster who will coordinate with the TRADOC webmaster webmaster@monroe.army.mil), the mission PAO, OPSEC officer, and SJA. PAOs must clear information for posting on public web sites. When requested by PAOs, the OPSEC officer and SJAs will assist in information reviews. TRADOC personnel will not make Privacy Act or Freedom of Information Act (FOIA)-exempt information accessible using public web sites.

(2) AKO Organizational Portals. Organizational portals will be created under the appropriate TRADOC organization as detailed in TR 10-5 series. Organizations desiring to create a new portal will coordinate with the TRADOC AKO administrator. Organizational portal administrators are responsible for the organizational structure under them to include authorizing and creating of sub-communities and knowledge centers. Sub-community administrators are responsible for notifying the next higher organization level administrator of changes in personnel and for maintenance of the structure under them.

d. Restricted Access Portals. Administrators are responsible to ensure all content inappropriate for public viewing is located behind AKO or the approved TRADOC knowledge environment. Restricted access by domain or Internet Protocol address only (i.e., .mil restricted) is not sufficient for content inappropriate for public viewing. Once an administrator has been designated, the administrator of the portal is responsible for assigning all other rights/permissions for users granted access. There are several options for restricted access portals in TRADOC: AKO Team Sites, TKE, and BCKS.

5.6. Publications.

a. Administrative Publications. TRADOC Regulation (TR) 25-35, Preparing and Publishing U.S. Army TRADOC Administrative Publications, details the responsibilities, policies, and procedures for preparing, publishing, and managing TRADOC administrative publications. TR 25-35 applies to all elements of TRADOC authorized to promulgate command-wide policy.

b. Training and Doctrine Publications. TR 25-36, Preparing and Publishing Training and Doctrinal Literature, details responsibilities, policies, and procedures for preparing, publishing, and managing training and doctrine publications.

Chapter 6
Network Operations.

6-1. DOIM-Provided Infrastructure. The IMA provides common user baseline services (e.g., NIPRNET and SIPRNET, e-mail, file storage, print, web, and domain services) for all Army organizations located on installations or in the immediate supporting area of an Army installation. The IMA may host mission servers/services on a reimbursable basis when arranged through a service level agreement. TRADOC organizations coordinate with their supporting DOIM(s) where appropriate to ensure that any information infrastructure (e.g., networking and server environment), that is a required component of successful employment of planned IT, is available or programmed. TRADOC organizations coordinate installation and fielding of IM/IT with the supporting DOIMs, consistent with the guidance given in AR 25-1. TRADOC CIO will assist TRADOC organizations in the resolution of infrastructure issues, e.g., with IMA or NETCOM that cannot be resolved locally.

6-2. Mission Support. Common and mission servers will be consolidated or eliminated where operationally possible in order to lower the total cost of ownership. TRADOC will centralize mission IM/IT services in common hosting facilities under the supervision of an approved service provider, when feasible. TRADOC elements with new or emerging requirements for IM/IT services will report them via the RAD form. When planning for new requirements, incorporate maximum use of existing Army and TRADOC capabilities before considering alternative solutions. Mission servers will be kept to a minimum and be reported in the TCAR.

6-3. Network Access.

a. Except where USAAC provides community of interest network access via other means, TRADOC activities will maximize the use of NETCOM/DOIM-provided network access services. TRADOC activities will not circumvent or duplicate the network access architecture the supporting DOIM operates and maintains.

b. TRADOC organizations will access the Internet only through the DoD-operated wide area networks. TRADOC organizations will not acquire services from commercial Internet service providers without meeting requirements of AR 25-1. All web sites and web-enabled applications will be hosted on Army or DoD-operated systems. USAAC recruiting and cadet command units will coordinate with USAAC CIO for alternate means of support/access (i.e., VPN) if DoD networks are unavailable at their location.

c. TRADOC personnel and students who use personal home computers to access government sites for work or professional development, e.g. Outlook Web Access, Distance Learning, AKO, may require common access card cryptographic log-on to access these sites. Organizations are authorized to issue common access card readers and middleware purchased at government expense for home use. This equipment is government property and will be returned when no longer needed. CIO/G6 or IMOs will coordinate with the local DOIM for installation.

d. TRADOC permits the provision of network services for telework. TRADOC Regulation 600-18 prescribes TRADOC's general policies for telework. Information Management Officers will coordinate provision of network services to teleworkers with the supporting DOIM and Information Assurance Manager.

6-4. Wireless Networking. Wireless networking removes the encumbrance of wire connections on portable devices and provides users the ability to travel beyond traditional network boundaries without losing network connectivity. Organizations desiring to implement wireless solutions must submit requirements via the RAD form and develop the business case that identifies cost benefit, security, operational necessity. Until the IMA provides wireless as a baseline service, TRADOC organizations must program funding for this network capability. Wireless local area network solutions must be implemented IAW the policies and procedures in AR 25-2 and Army's Wireless Security Standards Best Business Practice. Mobile users will comply with requirements in the "Road Warrior" Laptop Security Best Business Practice. (https://informationassurance.us.army.mil)

6-5. Messaging.

a. The DMS is the record messaging system for all organizations in DoD. TRADOC activities that require the use of official organizational messaging will use DMS. Any message that commits resources, directs action, clarifies official position, or issues official guidance is an organizational message.

b. TRADOC organizations will implement the number of DMS organizational accounts required to accomplish their missions. Since DMS does not support individual accounts, TRADOC organizations will coordinate with their supporting DOIM to establish DMS accounts and to ensure they are correctly listed in the Army Directory Information Tree. Each HQ TRADOC staff section and other TRADOC activities will have at least one unclassified organizational account. Locate the organizational account on one personal computer that will serve as a common user workstation to send/receive DMS messages. Incoming messages are distributed from the common user workstation to appropriate subordinate organizations.

c. TRADOC organizations will coordinate with their supporting DOIM to obtain certificates (Fortezza cards) for their organizational accounts.

6-6. Appropriate Use of Communications Systems. The use of TRADOC communications systems involving e-mail is limited to the conduct of official business or other authorized uses as defined in AR 25-1, chapter 6.

a. Official business as it concerns e-mail message use is defined as those necessary in the interest of the government (for example, e-mail messages that directly relate to the conduct of DoD, DA, or TRADOC business or that have an indirect impact on the command's ability to conduct its business). Signature blocks for official e-mail messages

should only include the sender's name, title, organization, phone, fax, and e-mail address. Unless as otherwise noted below, unofficial logos, sayings, quotations, mottos, slogans, or similar messages or attached unofficial pictures or files are not permitted for use in official e-mail traffic, either as part of the signature block or located elsewhere within the official e-mail message. The only exception for the conduct of official business involving e-mails is the inclusion of recognized unit or TRADOC organizational mottos or logos (such as "Victory Starts Here!").

b. Authorized use (as opposed to official use) e-mail messages are not similarly restricted by format concerns as it relates to the use of logos, sayings, quotations, mottos, slogans, or similar messages; however, there are prohibitions in place regulating the conduct of authorized use of e-mail for unofficial purposes. Prohibited use of TRADOC communications systems include:

(1) the use of communications systems that would adversely reflect on DoD, DA, or TRADOC (such as those involving sexually explicit e-mail or pornographic images; chain e-mail messages; unofficial advertising, soliciting, or selling via e-mail; and other uses that are incompatible with public service).

(2) the use of communications systems for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or public laws (which may include, but is not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment); and

(3) political transmissions to include transmissions that advocate the election of a particular candidate for public office.

6-7. Command, Control, Communications & Computers (C4) Reporting. Commanders will ensure C4 degradations are reported in accordance with TRADOC Command Guidance 04-001.

Appendix A
References

Section I
Required Publications

AR 25-1
Army Knowledge Management and Information Technology

AR 25-2
Information Assurance

AR 25-30
The Army Publishing Program

AR 25-400-2
The Army Records Information Management System (ARIMS)

DA PAM 25-1-1
Information Technology and Support Services

Section II
Related Publications

DoD Instruction 5000.2
Operation of the Defense Acquisition System

DFAS-IN Reg 37-1
Finance and Accounting Policy Implementation
(https://dfas4dod.dfas.mil/centers/dfasin/library/ar37-1/)

AR 5-14
Management of Contracted Advisory and Assistance Services

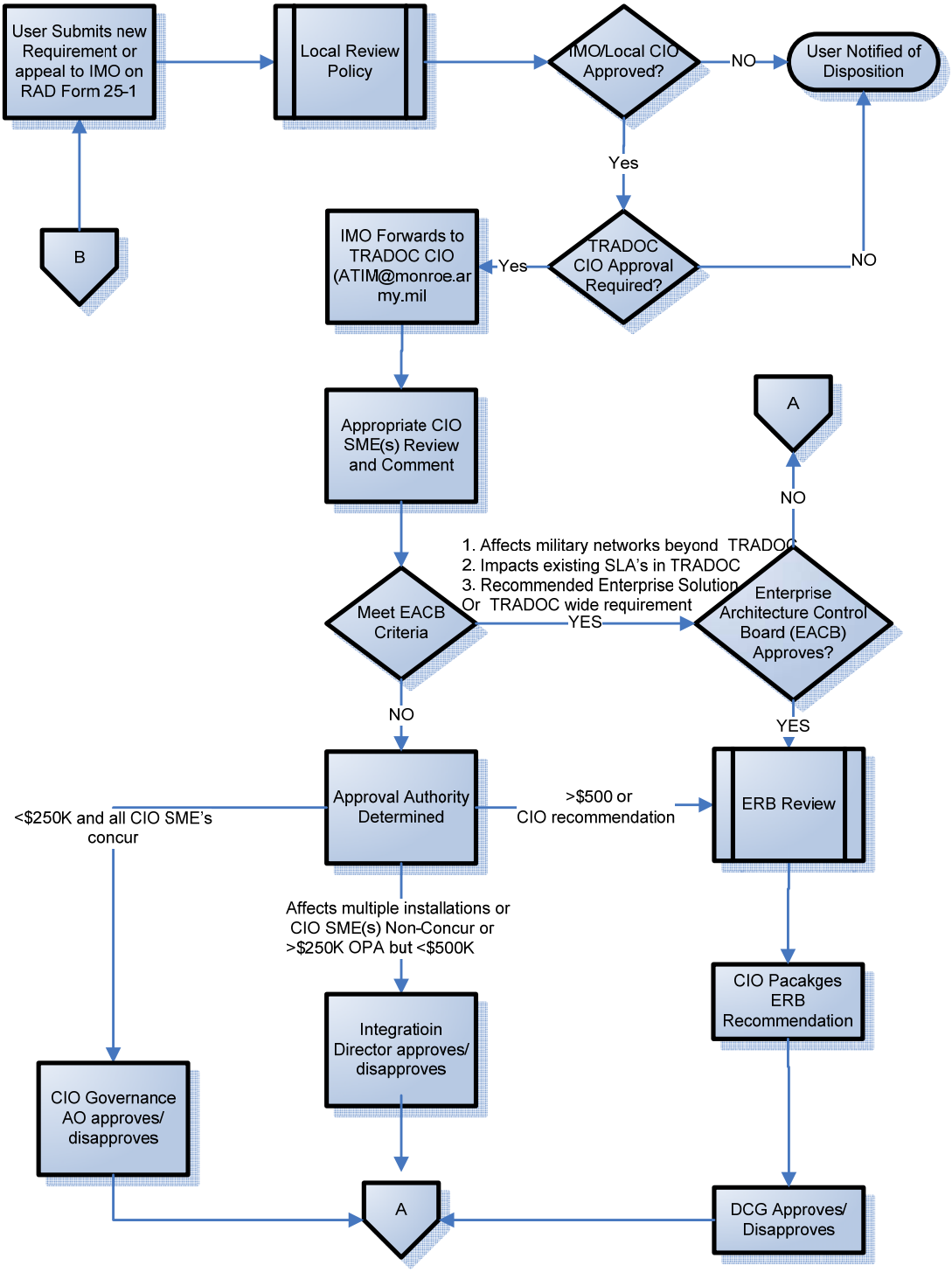
TR 10-5
U.S. Army Training and Doctrine Command

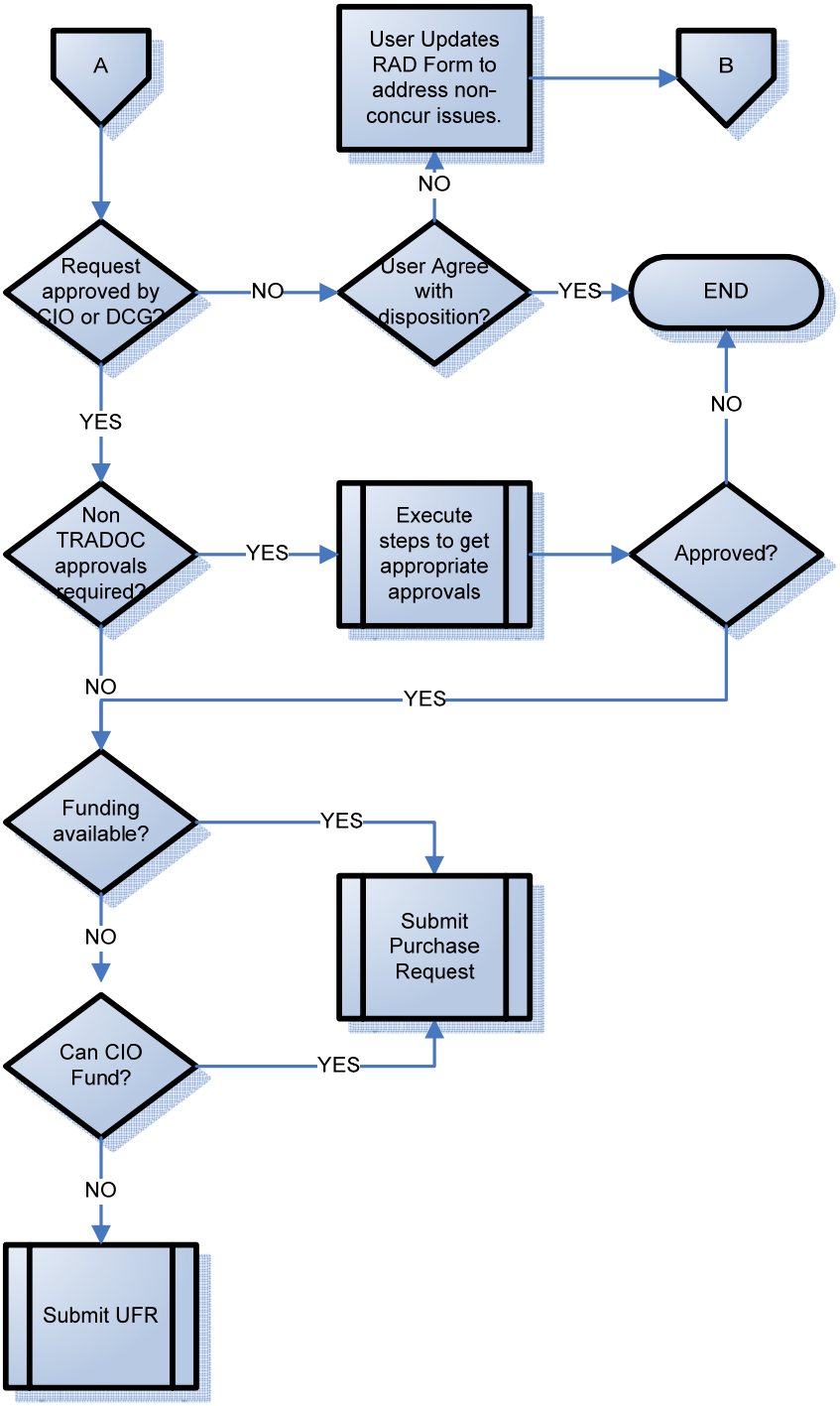
DoD Directive 8500.1,
Information Assurance (IA)

DoD Instruction 8500.2
Information Assurance (IA) Implementation

Appendix B

Governance Process




A
User Updates RAD Form to address non-concur issues.
B
NO
Request approved by CIO or DCG?
NO
User Agree with disposition?
YES
END
YES
NO
Non TRADOC approvals required?
YES
Execute steps to get appropriate approvals
Approved?
NO
YES
Funding available?
YES
Submit Purchase Request
NO
Can CIO Fund?
YES
NO
Submit UFR

Appendix C
Metadata and Taxonomies

Department of Defense Directive 8320.2 – Data Sharing in a Net-Centric Department of Defense, establishes policy and responsibilities to implement data sharing and to make data visible, accessible, and understandable.

The DDMS defines discovery metadata elements for resources posted to community and shared spaces. The DDMS specifies a set of information fields that are to be used to describe any data or service assets that are to be made known to the DoD Enterprise. The most recent version of DDMS will be employed consistently across the department's disciplines, domains, and data formats.

DDMS Tags (*Mandatory):

- Security* - The highest level of classification.
- Title* - A name given to the content resource.
- Identifier* - An example of an identifier is a URL or standard serial number.
- Creator* - An entity primarily responsible for making the content of the resource, i.e. author.
- Publisher – The entity responsible for posting the authoritative content.
- Contributor – An entity responsible for making contributions to the content of the resource.
- Date – A date of an event in the lifecycle of the resource (YYYY-MM-DD).
- Rights – Information about rights held in and over the resource (e.g., copyright or intellectual property rights).
- Language – A language of the intellectual content of the resource.
- Type – Name of the taxonomy schema used.
- Source – A reference to the original resource from which the present resource is derived.
- Subject* - Topic(s) of the content of the resource.
- Geospatial Coverage* - Geographic place names or coordinates that relate to the resource, mandatory unless not applicable.
- Temporal Coverage* - Subject matter coverage expressed in terms of one or more periods of time, mandatory unless not applicable.
- Virtual Coverage – The subject matter coverage of a publication in terms of one or more virtual addresses.
- Description – A summary of the content.
- Format – The physical or digital manifestation/media type of the resource (i.e., video, mime, Word document, etc).

Glossary

Section I
Abbreviations

ACA	Army Contracting Activity
AEI	Army Enterprise Infostructure
AITR	Army Information Technology Repository
AKM	Army Knowledge Management
AKO	Army Knowledge Online
APMS	Army Portfolio Management Solution
AR	Army Regulation
ARCIC	Army Capabilities Integration Center
ARIMS	Army Records Information Management System
ASCP	Army Small Computer Program
AUTL	Army Universal Task List
BCKS	Battle Command Knowledge System
BMMP	Business Management Modernization Program
BPA	Blanket Purchase Agreement
CB	Consolidated Buy
CG	Commanding General
CIO	Chief Information Officer
COTS	Commercial Off-the-Shelf
DA	Department of the Army
DCG	Deputy Commanding General
DCSOPS&T	Deputy Chief of Staff for Operations and Training
DCSRM	Deputy Chief of Staff for Resource Management
DDMS	Department of Defense Discovery Metadata Specifications
DDOE	Defense Information Systems Agency Direct Order Entry
DFAS-IN	Defense Finance and Accounting Service, Indianapolis Center
DISN	Defense Information System Network
DMS	Defense Messaging System
DoD	Department of Defense
DOIM	Director(ate) of Information Management
DOS	Department of State
EA	Enterprise Architecture
EAP	Enterprise Architecture Plan
EAMB	Enterprise Architecture Management Board
ERB	Enterprise Review Board
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
HQ	Headquarters
HQDA	Headquarters, Department of the Army
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance

IAVM	Information Assurance Vulnerability Management
IAW	in accordance with
IM	Information Management
IMA	Installation Management Agency
IMO	Information Management Officer
IMSP	Information Management Strategic Plan
IS	Information System
IT	Information Technology
KM	Knowledge Management
LCR	Life Cycle Replacement
MRB	Mission and Resources Board
MSC	Major Subordinate Command
NETCOM	Network Enterprise Technology Command
NIPRNET	Nonsecure Internet Protocol Router Network
OMA	Operations Maintenance Army
OPA	Other Procurement Army
OPFAC	Operational Facilities
OPSEC	Operations Security
PAM	Pamphlet
PDA	Personal Digital Assistant
PPBES	Planning, Programming, Budgeting and Execution System
RAD	Reporting and Acquisition Decision
SBU	Sensitive But Unclassified
SIPRNET	Secure Internet Protocol Router Network
SJA	Staff Judge Advocate
SRC	Senior Resource Committee
TCAR	TRADOC CIO Architecture Repository
TKE	TRADOC Knowledge Environment
TR	TRADOC Regulation
TRADOC	Training and Doctrine Command
TTP	Tactics, Techniques and Procedures
UFR	Unfinanced Requirement
USAAC	United States Army Accessions Command
WebTAS	Web based TRADOC Automated Schedules

Section II
Terms

Authoritative Data Source
A source of data or information that is recognized to be valid or trusted because IM/IT is from an official release authority or an official publication or reference (i.e., regulation or doctrine).

Content Management
A set of processes and technologies that support the evolutionary life cycle of digital information.

Data Management
The process of creating a basis for posting, sorting, identifying, and organizing the vast quantities of data available to DoD. (AR 25-1)

Discovery
Services that enable the formulation and execution of processes to advertise (make visible) and locate data assets (e.g., files, databases, services, directories, web pages, streams) by exploiting metadata descriptions stored in and or generated by IT repositories (e.g., directories, registries, catalogs, repositories, other shared metadata storage) and other exposed product or service attributes.

disposition instructions
Precise instructions specifying the time or event for transfer, retirement, or destruction of records.

federated data
Data that is accessed across physical boundaries, which may be system to system, department to department, or enterprise to enterprise boundaries.

Information life cycle management
A comprehensive approach to managing the flow of an information system's data and associated metadata from creation and initial storage to the time when IM/IT becomes obsolete and is deleted.

Information Management (IM)
Planning, budgeting, manipulating, and controlling information throughout its lifecycle. (AR 25-1)

Information Technology (IT)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Also includes computers, audio visual, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (AR 25-1)

information services
Any service performed in support of information management. Included are automation, visual information, telecommunications, integrated information, and printing and publication support activities.

information system
Organized assembly of resources and procedures designed to provide information needed to execute or accomplish a specific task or function. Information system equipment consists of components (e.g., hardware, software, firmware, products, or other items) used to create record, produce, store retrieve, process, transmit, disseminate, present, or display data or information.

information system component
Hardware, software, firmware, products, procedures, or other items used in the assembly of information systems.

information system equipment
Equipment that is a configuration of one more information system components used for the creation, recording, production, storage, retrieval, processing, transmission, dissemination, presentation, or display of data or information. Information system equipment is used to perform functions associated with automation, telecommunications, visual information, printing, publishing, and records management in support of the Army's mission.

initiative
An IM/IT initiative is an effort with a sponsor and budget that has a defined scope with an estimated start date and an end date. Initiatives can be related to improvement efforts or implementation of a new system, technology, process, or service. Initiatives are not mandatory maintenance and repair or operational continuity/sustainment unless those costs were unforcasted or not part of the initial business case.

Knowledge Management (KM)
An approach to improving organizational outcomes and organizational learning by introducing into an organization a range of specific processes and practices for identifying and capturing knowledge, know-how, expertise and other intellectual capital, and for making such knowledge assets available for transfer and reuse across the organization.

long-term record
The designation applied to records that have value beyond the business process, such as for historical, lessons learned, or research purposes. This type of record is kept longer than 6 years.

Office Record List
A list of the specific record titles and/or numbers describing the records accumulated or generated in an office. The list is prepared within each element where records are accumulated or generated and should be coordinated with the organization or installation records management official.

Official Record
Official records include all documentary materials, regardless of physical form or characteristics, that provide evidentiary accounting for decisions, policies, plans, organizations, functions, procedures, operations, and essential transactions of an organization (as defined in 44 U.S.C. 3301).

Operational Facilities (OPFAC) Allocations
A set of guidelines that define functional elements (i.e., a generic duty positions such as action officer or senior executive, or a place such as a conference room) and apply assignment rules, allocation rules, and IM/IT requirements descriptions corresponding to the functional element. TRADOCs OPFAC guidelines are available on the AKO IT RAD portal.

Public web site
A web site that is accessible from the Internet and uses no positive access control, for example, user authentication or firewalls, to restrict access to the information posted on the web site. Web site is used to also include any network service that gives a persistent presence to information on the Internet, with or without a Hyper Text Transfer Protocol (HTTP) front end (for example, File Transfer Protocol (FTP) site).

Private web site
A web site that screens or challenges users prior to permitting access to the information posted on the site. Private web sites may be connected to an intranet (that is, users are screened from accessing the entire network) or the Internet (that is, users are screened before entry into the specific web site). The term 'web site' also includes any network service that gives a persistent presence to information on the Internet, with or without an HTTP front end (for example, FTP site).

permanent record
The designation applied to records worthy of permanent retention by the United States, and accessioned into the National Archives until the end of democracy.

record copy
That copy of a record kept by the agency, office, or element directly responsible for the function to which the record relates that has been identified as the copy to be maintained to document the action taken or business transacted. Record copies of incoming or outgoing communications may be in a variety of forms. These include electronic copy, paper copy, handwritten items, specific media, microforms, etc. IM/IT does not include reading file copies or copies held for convenience or reference.

Sensitive information
Any information the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of

Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes information in routine DoD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

(1) FOUO — in accordance with DoD 5400.7–R, information that may be withheld from mandatory public disclosure under the FOIA.

(2) Unclassified technical data — Data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DoDD 5230.25.

(3) Department of State (DOS) Sensitive But Unclassified (SBU) — Information originating from the DOS that is determined to be SBU under appropriate DOS information security polices.

(4) Foreign Government Information — Information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DoD 5200.1–R.

(5) Privacy data — Personal and private information (for example, individual medical information, home address and telephone number, and social security number) as defined in the Privacy Act of 1974. (AR 25-2)

Shareable Content Object Reference Model (SCORM)
An XML-based method for representing course structures. IM/IT enables the reuse of web-based learning content across multiple environments and products.

short-term record
The designation applied to records that have no value beyond the business process and usually not kept longer than 6 years.

total program costs
All expenditures for research, development, procurement, installation, and maintenance necessary to field a solution for a stated requirement.

warfighting requirements
Warfighting requirements are requirements for acquisition category I-IV weapons and materiel systems, automated information systems, IM/IT programs, special access programs, and clothing and individual equipment in direct use by or support of the Army warfighter in training for and conducting operational missions (tactical or other), or connecting that warfighter to the sustaining base. (AR 71-9)

FOR THE COMMANDER:

OFFICIAL:

THOMAS F. METZ
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff

RANDALL L. MACKEY
Colonel, GS
Chief Information Officer